UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/587,932	06/06/2000	Xin Qiu	D02308	8876

43471 7590 07/13/2007

GENERAL INSTRUMENT CORPORATION DBA THE CONNECTED
HOME SOLUTIONS BUSINESS OF MOTOROLA, INC.
101 TOURNAMENT DRIVE
HORSHAM, PA 19044

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
07/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/587,932	QIU ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-9,14-17 and 23-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-9,14-17 and 23-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-4, 6-9, 14-17, 23-26 are pending.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Arguments

Applicant's remarks submitted on 4/19/2007 were considered persuasive. The rejections made in the prior office action are withdrawn. However, please note new rejections below.

Claim Objections

Claims 14 and 23 are objected to because of the following informalities:

1. There should be a comma before the first "the" in line 7 of claim 14.
2. Line 9 of claim 23 should recite "said first set of decryption keys".
3. It is suggested that applicant consistently use either "said" or "the" when referring to the same item in a claim, i.e. see lines 8-10 of claim 23 which refers to both "said first-level-of-encryption" and "the first-level-of-encryption".
4. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 23 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 23 recites "said integrated circuit" and "said set-top box" in the last line, both of which lack antecedent basis.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 24-26 are rejected under 35 U.S.C. 102(b) as being anticipated by Gammie et al (US 5,381,481).

Claim 24:

Gammie discloses:

1. Storing a first set of decryption data associated with a first data stream (col 11, lines 10-13; col 12, lines 56-61; and col 13, lines 35-42), wherein the first data stream includes a first number of services (col 5, lines 40-59). *Each of the services encrypted using Gammie's invention was encrypted using a different encryption algorithm and key, thus for the device seen in Figure 5 to be able to undo each of the different types of encryption, it must have stored multiple different types of decryption algorithm and keys in memory.*

2. Receiving the first data stream wherein the first data stream has a first-level-of-encryption (Fig 4, step 90; Fig 6, step 130; col 9, lines 6-20; and col 9, line 67-col 10, line 3). *Note that different services were encrypted using different encryption algorithms/levels and sent to the decryption device seen in Figure 5.*
3. Decrypting the first data stream using the first set of decryption data (col 12, lines 12-16 and Fig 4, step 140).
4. Storing a second set of decryption data associated with a second data stream, wherein the second data stream includes a second number of services (col 11, lines 10-13; col 12, lines 56-61; and col 13, lines 35-42). *The device seen in Figure 5 is capable of decrypting data streams encrypted using different encryption algorithms, thus this means that it stored more than one type of decryption algorithm and keys.*
5. Receiving the second data stream wherein the second data stream has a second-level-of-encryption (Fig 4, step 90; Fig 6, step 130; and col 9, line 67-col 10, line 3).
6. Decrypting the second data stream using the second set of decryption data (col 12, lines 12-16 and Fig 4, step 140).
7. Utilizing a common memory to decrypt the first data stream and the second data stream (col 11, lines 10-13; col 13, lines 35-42; and Fig 5, items 52' and 122).

Claim 25:

Gammie further discloses wherein the first set of decryption data comprises at least one decryption key (col 11, lines 10-13; col 12, lines 12-16; and Fig 5, item 122).

Note that item 122 is a register used to store the seed generated by seed generator 112. The seed is used in decryption, thus is a decryption key data.

Claim 26:

Gammie further discloses wherein the second set of decryption data comprises at least one decryption key (col 11, lines 10-13; col 12, lines 12-16; and Fig 5, item 122).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-9, and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gammie et al (US 5,381,481) in view of Wasilewski et al (US 5,400,401)

Claim 1:

Gammie discloses:

1. Storing a first set of encryption data associated with a first data stream (col 5, lines 10-13, 40-59; col 6, lines 10-13 and 50-57; and col 9, lines 5-20). *Note that a system key, SK, and seeds which are generated to be used in the encryption of data streams are stored by Gammie's invention. The algorithms used to encrypt the data are also stored in the service encryptor(s) and in seed encryptor 50*

seen in Figure 2. For purposes of discussion, the examiner will refer to the digital video signal as the first data stream. It should be understood though that any of the other signals discussed in column 5, lines 40-59 can be considered the first data stream.

2. Encrypting the first data stream having a first-level-of-encryption (col 5, lines 27-39; col 7, lines 3-5; and col 9, lines 6-20).
3. Sending the first data stream to a destination device for decryption (Fig 4, step 90).
4. Storing a second set of encryption data associated with a second data stream (col 5, lines 10-13, 40-49; col 6, lines 10-13 and 50-57; and col 9, lines 5-20). *Each of the services is encrypted using a different algorithm and seed data. As such, there are multiple sets of encryption data stored by Gammie's invention, each one associated with a different data stream. For purposes of discussion, the examiner will refer to the digital audio signal as the second data stream. It should be understood though that any of the other signals discussed in column 5, lines 40-59 can be considered the second data stream as long as it is not already considered the first data stream.*
5. Encrypting the second data stream having a second-level-of-encryption, the first-level-of-encryption being different from the second-level-of-encryption (col 7, lines 3-5 and col 9, lies 6-20). *Since each data stream is encrypted with a different algorithm, the level of encryption for each stream is different.*

6. Utilizing a common memory to encrypt the first data stream at said first-level-of-encryption and to encrypt the second data stream at the second-level-of-encryption (col 7, lines 9-16 and col 9, lines 21-45). *Note that rather than having multiple components to implement each of the encryption algorithm as seen in Figure 2, Gammie discloses that it is within the scope of his invention that the different components seen in Figure 2 are implemented by shared units or even in a single CPU. Further, note that SK memory 52 is shared by all the encryption units.*
7. Sending the second data stream to the destination device for decryption (Fig 4, step 90).

Gammie does not explicitly disclose wherein the first data stream includes a first number of services. Gammie does not explicitly disclose wherein the second data stream includes a second number of services that is different from the first number of services. However, recall that for purposes of discussion, the examiner considers the digital video stream disclosed by Gammie as the first data stream and the digital audio service as the second data stream. Further, Wasilewski discloses a first data stream includes a number of services (Fig 9; col 11, lines 12-28; and col 13, lines 64-66). Note that a number of video services (V_1'...V_N') are combined by a multiplexer 114 seen in Figure 9 of Wasilewski into a video stream, i.e. video data packets 120. Each of these video services (V_1'...V_N') corresponds to the video service of a particular show or program (Fig 1). Wasilewski also discloses a second data stream includes a second

number of services that is different from the first number of services (Fig 9 and col 14, lines 62-66). Note that a number of audio services ($A_1'...A_N'$) are combined by multiplexer 110 as seen in Figure 9 into an audio stream. Each of these audio services ($A_1'...A_N'$) corresponds to the audio service of a particular program or show (Fig 1). The video stream 120 and audio stream 122 is then encrypted using global encryptor 128 (col 15, lines 20-29).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Gammie and Wasilewski to arrive at the invention as claimed in claim 1. One skilled would have done so by encrypting a video stream made by multiplexing the video services of multiple programs as taught by Wasilewski using a first level of encryption as taught by Gammie. One skilled would also combine the two teachings by encrypting an audio stream made from multiplexing the audio services of multiple programs as taught by Wasilewski using a second level of encryption as taught by Gammie. One skilled would have been motivated to incorporate Wasilewski's teachings within Gammie's invention by multiplexing the number of services into a data stream because doing so ensures a more efficient use of system bandwidth (Wasilewski: col 2, lines 26-27).

Claim 2:

Gammie further discloses wherein the first set of encryption data comprises at least one encryption key (col 5, lines 27-32 and col 6, lines 50-57).

Claim 3:

Gammie further discloses wherein the destination device comprises a set-top box (Fig 5 and col 10, lines 57-59). The receiver seen in Figure 5 can be considered a set-top box since Gammie's invention can be used in a cable broadcast system.

Claim 4:

Gammie further discloses storing a plurality of decryption algorithms at the set-top box (col 12, lines 56-61).

Claim 6:

Gammie further discloses wherein the first-level-of-encryption utilizes the Data Encryption Standard and wherein the second-level-of-encryption utilizes an encryption algorithm different from said Data Encryption Standard (col 7, lines 1-8).

Claim 7:

Gammie further discloses decrypting the first data stream at the set-top box; and decrypting the second data stream at the set-top box (Fig 6, steps 136 and 140).

Claim 8:

Gammie does not explicitly disclose storing a portion of the first set of encryption data in a RAM. However, official notice is taken that storing encryption data within RAM was well known in the art of computing at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify Gammie's invention such that instead of using the registers (Fig 2, items 44, 46, and 48) to store a portion of the first set of encryption data, one instead used RAM. One skilled would have been motivated to do so because RAM is typically used to store most working data for a CPU.

Note that Gammie discloses that his invention can be implemented via use of a CPU (col 9, lines 37-45).

Claim 9:

Gammie further discloses storing a portion of the first set of encryption data in a register of a microprocessor (col 9, lines 37-45).

Claim 14:

Gammie discloses:

1. Allocating a memory with at first set of decryption data corresponding to a first-level-of-encryption (col 11, lines 10-13 and 29-37; col 12, lines 56-61; and col 13, lines 35-42). *Note that a decryption seed is generated by seed generator 112 seen in Figure 5. Since the encryption device utilizes different encryption algorithms to encrypt different data streams, the decryption device of Gammie's invention also must load different decryption algorithms into active memory.*
2. Receiving from an originating source a first data stream having the first-level-of-encryption, the second set of decryption data corresponding to said second-level-of-encryption (col 9, line 67-col 10, line 3; Fig 4, step 90; and Fig 6, step 130). *Note that the encryption device of Gammie's invention sends over multiple data streams which have differing levels of encryption. As such, the decryption device would receive multiple data streams having different levels of encryption.*
3. Re-allocating the memory with a second set of decryption data corresponding to a second-level-of-encryption, the second-level-of-encryption being different from

the first-level-of-encryption (col 12, lines 42-61; col 13, lines 35-42; and Fig 6, steps 136-144). *Note that the decryption device can be implemented via a CPU. The CPU must be able to decrypt data having different levels of encryption. As such, the CPU must be able to allocate and re-allocate memory with appropriate sets of decryption data for each different encryption algorithms and levels.*

4. Receiving from the originating source a second set of data stream having the second-level-of-encryption (col 9, line 67-col 10, line 3; Fig 4, step 90; and Fig 6, step 130).
5. Storing in memory said first set of decryption data corresponding to a first-level-of-encryption (col 11, lines 56-61; col 12, lines 56-61; and col 13, lines 35-42). *The decryption device must be able to decrypt data that has been encrypted by different encryption algorithms, thus there must inherently be stored in memory decryption data corresponding to each decryption algorithms.*

Gammie does not explicitly disclose the first data stream having a first number of services. Gammie also does not explicitly disclose the second data stream having a second number of services different from the first number of services. However, as discussed in the rejection of claim 1, these limitations were disclosed by Wasilewski. At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Gammie's invention using Wasilewski's teachings according to the limitations recited in claim 14. One skilled would have been motivated to incorporate Wasilewski's teachings such that the first data stream had/includes a first

number of services and the second had/includes a second number of services different from the first number of services for the same reasons discussed in claim 1.

Claim 15:

Gammie further discloses detecting that the second-level-of-encryption of the second data stream is different from the first-level-of-encryption of the first data stream (col 12, lines 56-61). The invention must be able to detect that a first data stream has a different level of encryption than a second data stream to be able to properly decrypt the each data. That is it must be able to detect that the algorithm needed to decrypt a first stream is different from what is needed to decrypt a second stream.

Claim 16:

Gammie further discloses wherein the allocating a memory with a first set of decryption data corresponding to the first-level-of-encryption comprises storing decryption key data (col 11, lines 10-13; col 12, lines 12-16; and Fig 5, item 122). Note that item 122 is a register used to store the seed generated by seed generator 112. The seed is used in decryption, thus is a decryption key data.

Claim 17:

Gammie further discloses wherein the re-allocating the memory with a second set of decryption data corresponding to said second-level-of-encryption comprises storing decryption key data (col 11, lines 10-13; col 12, lines 12-16; and Fig 5, item 122).

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al (US 5,400,401) in view of Gammie et al (US 5,381,481)

Claim 23:

Wasilewski discloses:

1. Providing a first set of services comprising a first number of services (Fig 9; col 11, lines 12-28; and col 13, lines 64-66). *Note that there are a number of video services associated with different programs.*
2. Encrypting at least one of said services from said first said first set of services (col 13, lines 18-20).
3. Combining the first set of services into a first data stream (Fig 9; col 11, lines 12-28; and col 13, lines 64-66).
4. Transmitting said first data stream (col 17, lines 12-25).
5. Providing a second set of services comprising a second number of services different from the first number of services (Fig 9 and col 14, lines 62-66). *Note that there are a number of audio services associated with different programs.*
6. Encrypting at least one of said services from said second set of services with an encryption algorithm (col 13, lines 18-20).
7. Combining the second set of services into a second data stream (Fig 9 and col 14, lines 62-66).
8. Transmitting said second data stream (col 17, lines 12-25).

Wasilewski does not explicitly disclose the at least one of said services from said first set of services are encrypted at a first-level-of-encryption while the at least one of said services from said second set of services are encrypted using an encryption algorithm different from said first-level-of-encryption. Wasilewski does not explicitly disclose storing a first set of decryption keys associated with said first-level-of-encryption, said first set of decryption keys corresponding to the decryption algorithm for said first-level-of-encryption. Wasilewski does not explicitly disclose storing a second set of decryption keys associated with said second-level-of-encryption in an integrated circuit in a set-top box.

However, Gammie disclose at least of one service from a first set of services is encrypted at a first-level-of-encryption while at least one of service from a second set of services are encrypted using an encryption algorithm different from said first-level-of-encryption (col 7, lines 3-5 and col 9, lines 6-20). Note that Gammie discloses several services (col 5, lines 40-59) and each of those services are encrypted using a different algorithm, thus each of the services are encrypted at a different level of encryption.

Gammie further discloses storing a first set of decryption keys associated with said first-level-of encryption, said first set of decryption keys corresponding to the decryption algorithm for said first-level-of-encryption and storing a second set of decryption keys associated with said second-level-of-encryption in an integrated circuit in a set-top box (Fig 5; col 11, lines 10-13; col 12, lines 56-61; col 13, lines 35-42). Note that the device seen in Figure 5 is considered a set-top box. It contains several

memories (at least items 52' and 122) which store values used in decryption of the received data streams containing the services. The data streams were encrypted with different levels of encryption.

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Wasilewski's invention according to the limitations recited in claim 23 in light of Gammie's teachings. One skilled would have been motivated to incorporate Gammie's teachings of different levels of encryption for a first and second set of services because Gammie discloses that television operators sometime may want to encrypt certain services more strongly than others (col 9, lines 6-12).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100